

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Hidema Tanaka et al.

Serial No.: 10/622,722

Filed: July 18, 2003

For: CIPHER STRENGTH ESTIMATING

DEVICE

Examiner: TBD

Group Art Unit: TBD

April 14, 2004

Irvine, California 92614

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

Dear Sir:

In an attempt to fully comply with the duty of disclosure set forth in 37 C.F.R. § 1.56 and in conformance with 37 C.F.R. §§ 1.97 (b)(3) and 1.98, applicant wishes to bring to the attention of the U.S. Patent Office the following references:

- L. Knudsen, "Truncated and Higher Order Differentials," Fast Software Encryption: 2nd International Workshop, Leuven, Belgium (December 14-16, 1994), LNCS 1008, pp. 196-211, Springer-Verlag.
- X. Lai, "Higher Order Derivatives and Differentia Cryptanalysis," R³ Security Engineering AG Ch-8607 Aathal, Switzerland, pp. 1-7; Reprint of pp. 227-233, "Communications and Cryptography," (Ed. R Blahut et al.), Kluwer Academic Publishers (1994).
- M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, *Fast Software Encryption: 3rd International Workshop*, Cambridge, UK (February 21-23, 1996), LNCS. 1039, pp. 205-218.
- S. Moriai, T. Shimoyama, T. Kaneko, "Higher Order Differential Attack of a CAST Cipher, Fast Software Encryption: 4th International Workshop, LNCS 1372, pp. 17-31.

A copy of these references and form PTO-A820 are attached.

If the Examiner believes that a telephone conference would help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

The Director is authorized to charge Deposit Account No. 19-2814 any filing fees which may be required.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 14, 2004, 2004.

By:

Lames Lea

Signature

Dated: April 14, 2004

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price

Resistration No. 25,124

1920 Main Street, Suite 1200 Irvine, California 92614-7230

Telephone: (949) 253-4920

Substitute For	m PTO-1449	J.S. Depa	Attorney's Docket No.		Application No.				
(Modified)	AP AP	Patent a	43521-0700		10/622,722				
	THE STATE OF THE S	A RANGE	Applicant Tanaka et al.						
	Informa		Filing Date		Group Art Unit				
		by Applicant several sheets if necessary)	July 18, 2003		TBD				
(37 CFR §1.9	8(b)) 								
			U.S. Paten	t Documents	, 		T		
Examiner Initial	Desig. ID	Patent Number	Issue Date	Patentee	Class	Subclass	Filing Date If Appropriate		
		.							
-	1			· · · · · · · · · · · · · · · · · ·			1		
								···-	
							-		
							<u> </u>		
	_								
	T			olished Foreign Pa	tent Ap	plications			
Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes No		
miciai	ID	Trumber	Dute	Tutont Office	Class	Subciuss	103	110	
				· · · · · · · · · · · · · · · · · · ·					
			· · · · · · · · · · · · · · · · · · ·		ļ			!	
Other Documents (include Author, Title, Date, and Place of Publication)									
Examiner Desig. Initial ID		Document							
Illitiai	10	L. Knudsen, "Trunc	nudsen, "Truncated and Higher Order Differentials," Fast Software Encryption: 2 nd						
	International Workshop, Leuven, Belgium (December 14-16, 1994), LNCS 1008, pp. 196-2							1,	
		Springer-Verlag. X. Lai, "Higher Order Derivatives and Differentia Cryptanalysis," R ³ Security Engineering AG Ch-							
		8607 Aathal, Switze	erland, pp. 1-7; R	eprint of pp. 227-233, "	rint of pp. 227-233, "Communications and Cryptography,"				
		(Ed. R Blahut et al.)	(Ed. R Blahut et al.), Kluwer Academic Publishers (1994). M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear						
	M. Matsui, "New Structure of Block Cipners with Provable Security against Differential and Line Cryptanalysis, Fast Software Encryption: 3 rd International Workshop, Cambridge, UK (February								
	21-23, 1996), LNCS. 1039, pp. 205-218.								
,		S. Moriai, T. Shimoyama, T. Kaneko, "Higher Order Differential Attack of a CAST Cipher, Fast Software Encryption: 4th International Workshop, LNCS 1372, pp. 17-31.							
Signature	1	1 = 5,7 2.2		Date Considered	, FF. • .				
EXAMINER: communication			ough citation if not in	n conformance and not consid	lered. Includ	le copy of this for	m with next		